

In the United States Patent and Trademark Office

028410-0002 DIV

In re Application of:

Inventor(s): Balas Natarajan Kausik, Ph.D.

Serial No.: Not Yet Assigned

Filing Date: December 27, 2000

Title: Computer-Readable Medium  
Having a Private Key  
Encryption Program

which is a divisional of application:

Serial No.: 08/996,758

Filing Date: December 23, 1997

Title: Method and Apparatus for  
Cryptographically Camouflaged  
Cryptographic Key Storage,  
Certification and Use

Art Unit: 2766

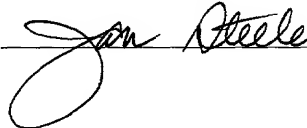
Examiner: Dr. Pinchus M. Laufer

**CERTIFICATE OF MAILING BY "EXPRESS MAIL"**

"Express Mail" Mailing Label Number: EK 447 202 151 US  
Date of Deposit: December 27, 2000

I hereby certify that this paper and all enclosures are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" under 37 CFR § 1.10 on the date indicated above and are addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Type or Print Name of Person Mailing: Jan Steele



**PRELIMINARY AMENDMENT**

Assistant Commissioner for Patents  
Box Patent Application  
Washington, D.C. 20231

Sir:

Prior to examination of the above-referenced divisional patent application, please enter the following amendments and consider the following remarks.

## AMENDMENT

### In the Specification:

- A. On page 1, amend the title as follows:  
delete "METHOD AND APPARATUS FOR SECURE CRYPTOGRAPHIC KEY  
STORAGE, CERTIFICATION AND USE" and insert – COMPUTER-READABLE  
MEDIUM HAVING A PRIVATE KEY ENCRYPTION PROGRAM – therefor.
- B. On page 1, before "**FIELD OF THE INVENTION**," add:  
– **RELATED APPLICATION**  
This application is a divisional of U.S. patent application serial number  
08/996,758, filed on December 23, 1997. –
- C. On page 10, line 8, after "**DETAILED DESCRIPTION OF THE INVENTION**," add:  
– Copending U.S. patent application serial no. 08/996,758 is hereby incorporated by  
reference. –

### In the Claims:

- A. Please cancel original claims 1-97 without prejudice.
- B. Please add new claim 1 as follows:
- 1.(New) A computer-readable medium comprising a program for encrypting a private key  
used in cryptography, the program being executable on a computer to carry out  
the steps of:  
dividing an exponent of the private key into a most significant portion and  
a least significant portion;  
encrypting the least significant portion; and


combining the most significant portion, without encryption, and the encrypted version of the least significant portion, and storing the combined portions as the encrypted private key.

### REMARKS

Support for the new claim is found on page 15, last paragraph of the original specification. If the Examiner has any questions or concerns, he is invited to call the Applicant's attorney, Fred Kim, at (650) 470-4618.

Respectfully submitted,

Date: December 27, 2000

  
Frederick D. Kim, Ph.D.  
Registration Number 38,513

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP  
525 University Avenue  
Palo Alto, California 94301  
Telephone: (650) 470-4500  
Facsimile: (650) 470-4570